JOURNAL OF NUMBER THEORY **56**, 329–335 (1996)
ARTICLE NO. 0022

Remarks on a Paper of Wagner

Soon-Mo Jung and Bodo Volkmann

Mathematisches Institut A, Universität Stuttgart, Pfaffenwaldring 57, D-70569 Stuttgart, Germany

Communicated by Alan C. Woods

Received August 26, 1994

TO THE MEMORY OF GEROLD WAGNER

existence of such rings was shown in 1989 by Wagner for the case when g is a proper odd prime divisor of h with $(g,(h/g))=1$. This result is generalized to the case of arbitrary pairs of integers g, h with $g \mid h$ such that there exists a prime p_1 with $p_1 \nmid g$, $p_1 \mid (h/g)$.

1. Introduction

Throughout this paper let g and h be integers greater than 1. We call a real number a *Cassels-Schmidt number*, or *CS-number* for short, of the type $(g; h)$ if it is normal to base g but non-normal to base h. If we define the equivalence relation $g \sim h$ by requiring that $g^n = h^m$ for some $m, n \in \mathbb{N}$ then the well-known Cassels-Schmidt Theorem (for the history see, e.g. Volkmann [5] and the literature cited there) states that the set $CS(g; h)$ of such CS-numbers is non-empty if and only if $g \not\sim h$.

The original existence proofs by Cassels (1959) for the case $h=3$, $g \not\sim h$, and by Schmidt (1960) for the general assertion as well as subsequent sharpenings and extensions all used non-constructive, measure-theoretic methods until the first explicit examples of CS-numbers were exhibited and identified as such by the late Wagner ([6], [7]) in 1989. He was even able to show that for certain pairs g, h there exist rings W of real numbers with

$$W \setminus \{0\} \subseteq CS(g; h). \tag{1}$$

Therefore we will call any ring satisfying (1) a *Wagner ring* of the type $(g; h)$.

0022-314X/96 $12.00

Specifically, G. Wagner proved that, if g is an odd prime satisfying

$$g \mid h, g < h, \tag{2}$$

and

$$\left(g, \frac{h}{g}\right) = 1 \tag{3}$$

and if $\alpha(n)$, $\beta(n)$ are strictly increasing sequences of natural numbers such that

$$\beta(n-1) = o\left(\frac{\alpha(n)}{n}\right) \tag{4}$$

and

$$\alpha(n) = o(\log \beta(n)), \tag{5}$$

then the set of numbers of the form

$$y = \prod_{n=1}^{\infty} \left(1 + \frac{\varepsilon_n}{P(n)}\right), \; P(n) = m^{\alpha(n)} g^{\beta(n)}, \; m = \frac{h}{g}, \; \varepsilon_n \in \{-1, 1\}, \tag{6}$$

generates (within $\mathbb{R}$) a Wagner ring W of type $(g; h)$.

Since 1989 the following extensions of this theorem have been obtained:

1.1. Kano [1] generalized the result by weakening condition (4) to

$$\beta(n-1) = o(\alpha(n)). \tag{7}$$

1.2. Kano and Shiokawa [3] established the existence of Wagner rings of type $(g; h)$ for arbitrary integers g (not necessarily a prime) and h satisfying (2) and (3).

1.3. Recently, Kano [2] exhibited a quite general class of CS-numbers of type $(g; h)$, again subject to the conditions (2) and (3), which contains, in particular, the non-zero elements of all the Wagner rings mentioned so far. However, these sets are not themselves rings in general.

2. Result

In the present paper we will prove the existence of Wagner rings of the type $(g; h)$ for any pair satisfying (2) and, instead of (3), the following conditions:[1]

$$\text{There exists a prime } p_1 \text{ with } p_1 \nmid g, p_1 \,\Big|\, \frac{h}{g}. \tag{8}$$

Thus our result reads as follows:

Theorem. *Let g, h be integers with* (2) *and* (8), *and let $\alpha(n), \beta(n)$ be sequences satisfying* (7) *and* (5). *Then the set of numbers of the form* (6) *generates a Wagner ring of type* $(g; h)$.

3. Proof of the Theorem

We will follow Wagner's proof as rewritten by the authors in [7], with the following modifications.

3.1. Clearly, Lemma G remains true with (7) instead of (4).

3.2. In the proofs of [7], Lemmas 1 and 2 the parameter p, as implicitly involved in the symbols $P(n)$, $P(\underline{n}; \underline{\mu})$, $S(N, v)$ and $S(N_1, N_2; v_1, v_2)$ has to be replaced by $m = h/g$.

3.3. In [7], Section 3.4 we substitute for Wagner's prime p the number m_1, defined as the largest divisor of m (see (6) above) with $(m_1, g) = 1$. Then, if we let $m = m_1 m_2$, there exists a smallest exponent k such that $m_2 \mid g^k$. Furthermore, condition (8) implies that $p_1 \mid m_1$ and hence $m_1 > 1$.

For the approximations $x_0(N, v)$ as defined in [7], (32) we need the following assertion.

Lemma 4. *If $v \in \{1, ..., \ell\}$ is given and N is sufficiently large then there is an integer $\eta(N, v) \neq 0$ such that*

$$x_0(N, v) = \frac{\eta(N, v)}{m_1^{\gamma(N, v)} g^{\delta(N, v)}}; \eta \in \mathbb{Z}; \gamma, \delta \in \mathbb{N}; m_1 \nmid \eta, g \nmid \eta, \tag{9}$$

where $\delta(N, v) = v(\beta(N) + k\alpha(N)) + \ell \sum_{i=1}^{N-1} (\beta(i) + k\alpha(i))$.

[1] Example: The case $g = 2$, $h = 12$ is covered by our result but not by those mentioned under 1.1 through 1.3.

Proof. It follows from the proof of [7], Lemma 3 that, for the number c under consideration,

$$\sum_{(n, \eta) \leqslant (N, v)} S(n; \mu) = \frac{c}{P(N)^v} \prod_{i=1}^{N-1} \frac{1}{P(i)^{\ell}} \quad (v = 1, ..., \ell)$$

(for the meaning of the symbols P and S see 3.2 above). Consequently, the number

$$x_0(N, v) = A(0) + \sum_{(n, \mu) \leqslant (N, \mu)} S(n; \mu)$$

can be written as a fraction with the denominator

$$(m_1 m_2)^{\gamma(N, v)} g^{\tau(N, v)},$$

where

$$\gamma(N, v) = v\alpha(N) + \ell \sum_{i=1}^{N-1} \alpha(i),$$

$$\tau(N, v) = v\beta(N) + \ell \sum_{i=1}^{N-1} \beta(i).$$

Rewriting this denominator as

$$m_1^{\gamma(N, v)} \left(\frac{m_2}{g^k}\right)^{\gamma(N, v)} g^{k\gamma(N, v) + \tau(N, v)},$$

we finally obtain an equation of the form

$$x_0(N, v) = \frac{\eta(N, v)}{m_1^{\gamma(N, v)} g^{\delta(N, v)}},$$

which proves the lemma.

With these adjustments, Lemma 3 of [7] remains valid.

3.4. The following lemmas serve to simplify Wagner's proof and furthermore, to fill a gap concerning the case $g = 2$ (which is not covered by Wagner's approach). For any two integers a and n with $(a, n) = 1$ we denote the *order* of a mod n by $\omega_a(n)$.

LEMMA 5. *Let $q \geqslant 2$ be an integer and let $p_1, ..., p_s$ be distinct primes not dividing q. Then there exist exponents $e_i = e_i(q, p_1, ..., p_s)(i = 1, ..., s)$ such that, for all $n_i \geqslant e_i (i = 1, ..., s)$, the number $m = p_1^{n_1} \cdots p_s^{n_s}$ satisfies*

$$\omega_q(m) = p_1^{n_1 - e_1} \cdots p_s^{n_s - e_s} \omega_q(p_1^{e_1} \cdots p_s^{e_s}).$$

Proof. See Korobov [4], Lemma 1.

LEMMA 6. *In the notation of Lemma 4 assume that, for a given $c \in \mathbb{Z}$, $c \neq 0$, there exists an index $i \in \{1, ..., s\}$ such that $n_i > e_i$ and $p_i^{n_i - e_i} \nmid c$. Then*

$$\sum_{j=1}^{\omega_q(m)} \exp\left(\frac{2\pi i c q^j}{m}\right) = 0.$$

Proof. See Korobov [4], Theorem 2. (The proof is based on Lemma 5).

3.5. For the proof of Wagner's assertion (b) (normality to base g of any number $x_0 \in W \backslash \{0\}$) we modify the decomposition [7], (41) by writing $m_2 = m/m_1$ (see (9) and 3.3 above for the definitions of m_1 and m_2), letting k be the least exponent[2] with $m_2 | g^k$, by defining (compare [7], (40) through (42))

$$\beta^* = \beta(n) + k\alpha(n),\ \beta = \beta(n),\ L = \ell \sum_{j=1}^{n-1} (\beta(j) + k\alpha(j)),$$

$$J_v = [v\beta, v\beta^* + L) \cap [1, N]\ (v = 0, ..., u),$$

$$I_v = [v\beta^* + L, (v+1)\beta)\ (v = 0, ..., \mu - 1),$$

$$I_\mu = [\mu\beta^* + L, N).$$

Clearly, $I_\mu = \varnothing$ if $N < \mu\beta^* + L$. With this decomposition of the index interval $[1, N]$ we again use the sets

$$\Omega(I) = \{g^t x_0(n, v) (\mathrm{mod}\ 1) : t \in I\},$$

noting that with the abbreviations $\gamma = \gamma(n, v)$ and $\eta = \eta(n, v)$ one has

$$\Omega(I_v) = \begin{cases} \{\eta g^j / m_1^\gamma : j = 0, 1, ..., \beta - vk\alpha(n) - L - 1\} \\ \qquad \text{for} \quad v = 0, 1, ..., \mu - 1, \\ \{\eta g^j / m_1^\gamma : j = 0, 1, ..., N - \mu\beta^* - L\} \\ \qquad \text{for} \quad v = \mu. \end{cases}$$

[2] The existence follows from the definition of m_1.

3.6. As the next step we need, for the reasons already stated, a new proof of the following proposition.

LEMMA 7. *The discrepancies of the sets $\Omega(I_v)$ satisfy*

$$D(\Omega(I_v)) = o(N)(v = 0, ..., \mu).$$

Proof. According to the theorem of Fermat–Euler one has by (9) and (5), again writing $\gamma = \gamma(n, v)$. the relation

$$\omega_g(m_1^\gamma) \leqslant m_1^\gamma \leqslant m_1^{v\alpha(n) + \ell \sum_{j=1}^{n-1} \alpha(j)} = o(\beta(n)) = o(N). \tag{10}$$

Furthermore, the euclidean algorithm furnishes remainders b_v with $0 \leqslant b_v < \omega_g(m_1^\gamma)$ and numbers $a_v \in \mathbb{N}_0$ such that

$$|I_v| = a_v \omega_g(m_1^\gamma) + b_v \qquad (v = 0, ..., u). \tag{11}$$

Combining (11) with the Erdös–Turán inequality (see [7], proof of Lemma 4), (10) and Lemma 5 we obtain

$$\begin{aligned} D(\Omega(I_v)) \leqslant & \sup_{0 \leqslant a < b \leqslant 1} \max_{1 \leqslant i \leqslant \omega_g(m_1^\gamma)} | a_v \\ & \times \#\{1 \leqslant t \leqslant \omega_g(m_1^\gamma) : g^t x_0(n, v) \in [a, b) (\mathrm{mod}\ 1)\} \\ & + \#\{i \leqslant t < i + b_v : g^t x_0(n, v) \in [a, b) (\mathrm{mod}\ 1)\} \\ & - (a_v \omega_g(m_1^\gamma) + b_v)(b - a)| \\ \leqslant & a_v D(\Omega([1, \omega_g(m_1^\gamma)])) + \max_{1 \leqslant i \leqslant \omega_g(m_1^\gamma)} D(\Omega([i, i + b_v))) \\ \leqslant & a_v c \left(\frac{\omega_g(m_1^\gamma)}{t} + \sum_{h=1}^{t} \frac{1}{h} \left| \sum_{j=1}^{\omega_g(m_1^\gamma)} \exp(2\pi i h \eta g^j / m_1^\gamma) \right| \right) + o(N), \end{aligned}$$

where $0 < c \leqslant 6$ is constant and $t \in \mathbb{N}$ is arbitrary. Therefore,

$$D(\Omega(I_v)) \leqslant a_v c \frac{\omega_g(m_1^\gamma)}{t} + o(N),$$

and thus the lemma follows in view of (10).

3.7. For the final part of the proof of assertion (b) (compare [7], paragraph following relation (49)) we now obtain again by an argument similar to the proof of [7], inequality (29), the relation

$$|x_0(n, v) - x_0| \leqslant \begin{cases} m^{-(1/2)\alpha(n)} g^{-(v+1)\beta(n)} & \text{for} \quad v = 0, ..., l-1, \\ m^{-(1/2)\alpha(n+1)} g^{-\beta(n+1)} & \text{for} \quad v = l. \end{cases} \tag{12}$$

By (12), the mod 1 distance between the points $g^t x_0(n, v)$ and $g^t x_0$ is for any $t \in I_v$, since

$$t \leqslant \begin{cases} (v+1)\,\beta(n) & \text{for} \quad v = 0, \ldots, l-1 \\ \beta(n+1) & \text{for} \quad v = l, \end{cases}$$

bounded from above by $m^{-\alpha(n)/2}$. Now the assertion $D(\omega_N) = o(N)$ follows as in [7].

3.8. The non-normality of a given number $x_0 \in W \backslash \{0\}$ to base $h = mg$ can be proved similarly as in [7], Section 4.3.

4. Open Problems

The following problems appear to be of interest:

4.1. Do there exist Wagner rings of arbitrary type $(g; h)$, $g \nsim h$? Or, at least some with $g \nmid h$?

4.2. How large is the class of all Wagner rings of given type? Does it possess an algebraic sructure?

4.3. The same questions may be asked for additive groups of CS-numbers.

References

1. H. Kano, A remark on Wagner's ring of normal numbers, Research Report KSTS/RR-91/005 (1991).
2. H. Kano, General constructions of normal numbers of Korobov type, *Osaka J. Math.* **30** (1993), 909–919.
3. H. Kano and I. Shiokawa, Rings of normal and non-normal numbers, *Israel J. Math.* **84** (1993), 403–416.
4. N. M. Korobov, Trigonometric sums with exponential functions and the distribution of signs in repeating decimals, *Math. Notes* **8** (1970), 831–837.
5. B. Volkmann, On the Cassels–Schmidt Theorem I, *Bull. Sci. Math.* (2) **109** (1984), 321–336.
6. G. Wagner, On rings of normal and non-normal numbers, Preprint No. 34, Laboratoire de Mathématiques, Marseille, 1989.
7. G. Wagner, On rings of numbers which are normal to one base but non-normal to another, *J. Number Theory* **54** (1995), 211-231.